Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

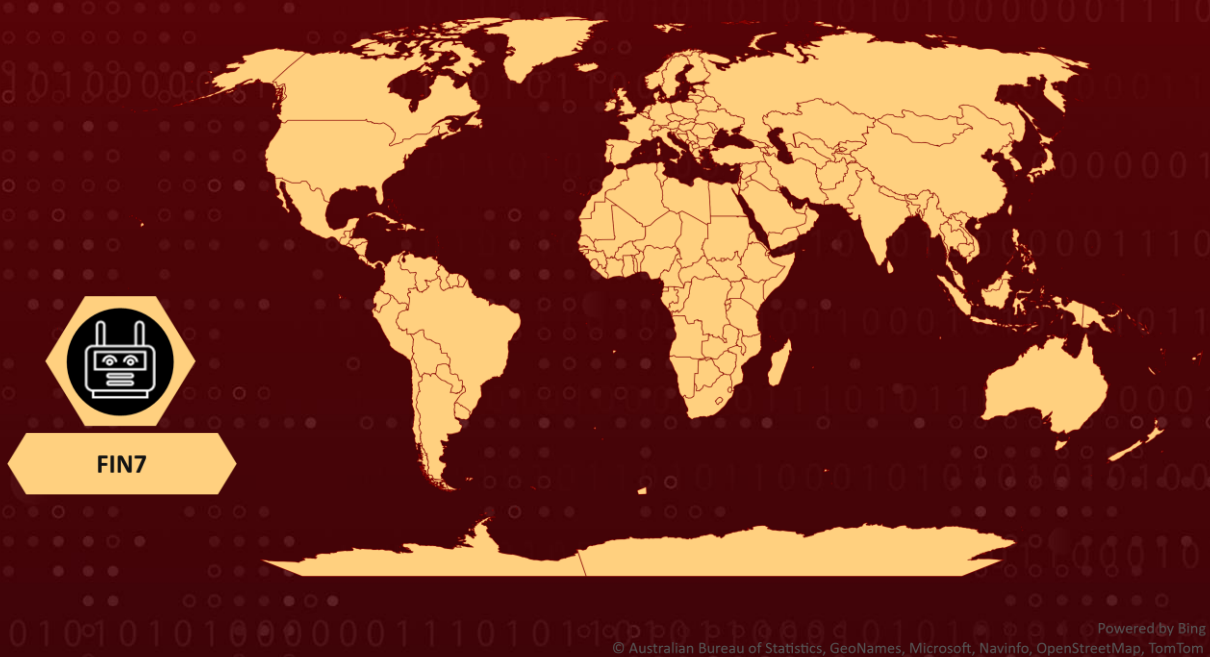
FIN7-Affiliated Hackers Exploit Flaws in Veeam Backup Servers

Date of Publication	Admiralty Code	TA Number
May 2, 2023	A3	TA2023207

Summary

Attack began: March 28, 2023
Actor: FIN7 (aka ITG14, Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, TAG-CR1)
Malware: POWERTRASH Loader & DICELOADER (also known as Lizar)
Attack Region: Worldwide
Attack: Publicly accessible servers using Veeam Backup & Replication (VBR) software were attacked, likely through a recently fixed vulnerability (CVE-2023-27532), by a group with similarities to the FIN7 activity group.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-27532	Veeam Missing Authentication for Critical Function	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition	✗	✗	✓

Attack Details

#1

Publicly accessible servers running Veeam Backup & Replication software have been targeted by intrusions. The attackers behind these incidents share characteristics with the FIN7 threat group. It is highly probable that the initial infiltration and execution of the attacks were made possible by exploiting a recently fixed vulnerability (CVE-2023-27532) in the Veeam Backup & Replication software.

#2

On March 28th, 2023, initial activity was detected on publicly accessible servers utilizing Veeam Backup & Replication (VBR) software, with approximately 7,500 VBR hosts still appearing vulnerable. A process associated with the Veeam Backup instance, known as "sqlservr.exe," launched a shell command that facilitated the in-memory download and execution of an obfuscated PowerShell script called "POWERTRASH."

#3

This POWERTRASH Loader script is associated with the FIN7 activity group and has been utilized to deploy various payloads, such as Carbanak, DICELOADER, and Cobalt Strike. The payload used in the March attacks was DICELOADER, also known as Lizar, which is a backdoor attributed to FIN7. The infiltrators used DICELOADER as a foothold to gain access to the compromised machines and carry out post-exploitation procedures.

Recommendations

Ensure that TCP port 9401 is not exposed to the internet or is protected by a firewall that only permits access to trusted IP addresses. Regularly review and monitor network activity for any suspicious or unauthorized connections, especially over port 9401.

Verify that all Veeam Backup & Replication software is up to date with the latest security patches to prevent exploitation of known vulnerabilities, such as CVE-2023-27532.

Consider implementing multi-factor authentication or other access controls to restrict unauthorized access to the backup infrastructure hosts. Educate employees and staff on the importance of strong password management practices and regularly rotating and updating credentials to minimize the risk of unauthorized access.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0007 Discovery	TA0008 Lateral Movement	TA0011 Command and Control	T1497 Virtualization/Sandbox Evasion
T1059 Command and Scripting Interpreter	T1566 Phishing	T1001 Data Obfuscation	T1047 Windows Management Instrumentation
T1059.001 PowerShell	T1010 Application Window Discovery	T1057 Process Discovery	T1083 File and Directory Discovery
T1071 Application Layer Protocol	T1573 Encrypted Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	8687b6b1508a93556d6e30d14e5c4ee9971f2d80 b621f8c5e9033718b4e9d47a2f0eccb9783f612a e5480a47172e3f75dbf0384f4ca82c7b47910e0f
IPV4	217[.]12.206.176 162[.]248.225.115 45[.]136.199.128 91[.]149.243.181 91[.]199.147.152 95[.]217.49.123 77[.]75.230.112 194[.]87.148.41 195[.]123.244.162

Patch Links

https://www.veeam.com/kb4424

References

https://labs.withsecure.com/publications/fin7-target-veeam-servers

https://github.com/WithSecureLabs/iocs/blob/master/FIN7VEEAM/iocs.csv

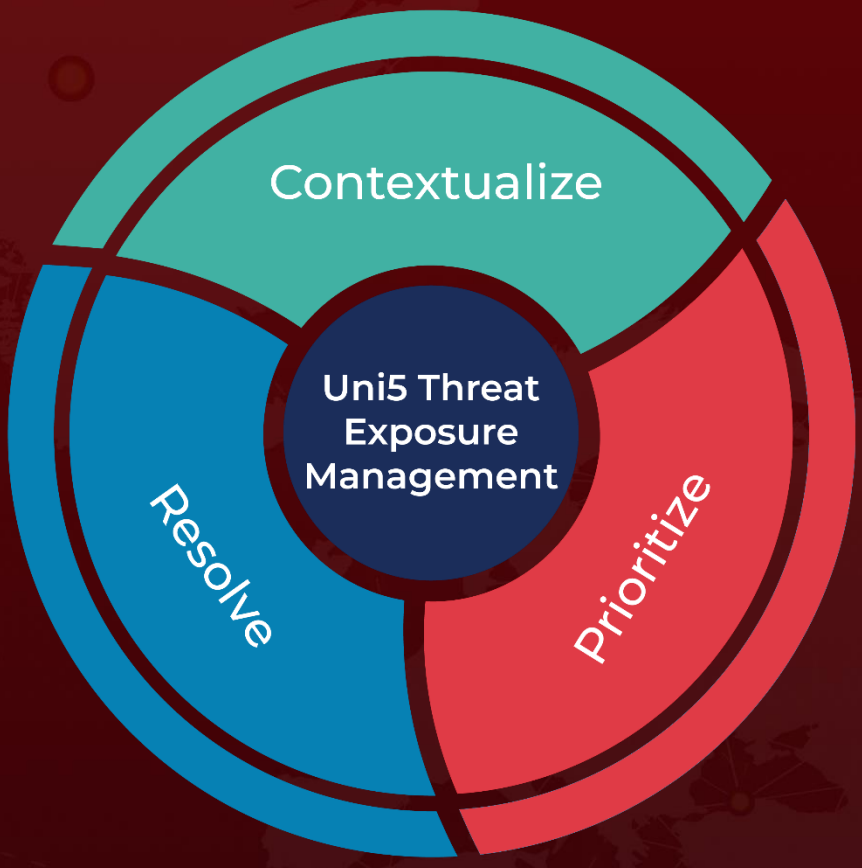
https://attack.mitre.org/groups/G0046/

https://github.com/horizon3ai/CVE-2023-27532

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 2, 2023 • 5:55 AM

More at www.hivepro.com